

## AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

- 1 1. (Currently Amended) A method of preventing an attack on a network, the method comprising the computer-implemented steps of:
  - 3 receiving an ICMP packet ~~that includes, wherein a data field within the ICMP packet includes a copy portion~~ of a header associated with a connection in a connection-oriented transport protocol, ~~and wherein the portion of the header includes a packet sequence value associated with the connection;~~
  - 7 obtaining [[a]] ~~the~~ packet sequence value from the header;
  - 8 determining if the packet sequence value is valid; ~~and~~
  - 9 responding to the ICMP packet by updating a parameter value associated with the
  - 10 transport protocol connection only if the packet sequence value is determined
  - 11 to be valid.
- 1 2. (Currently Amended) A method as recited in Claim 1, wherein the step of receiving an ICMP packet comprises receiving an ICMP packet that includes a ~~copy portion~~ of a TCP header associated with a TCP connection.
- 1 3. (Original) A method as recited in Claim 1, wherein the step of receiving an ICMP packet comprises receiving an ICMP “endpoint unreachable” error packet.
- 1 4. (Original) A method as recited in Claim 1, wherein the step of receiving an ICMP packet comprises receiving an ICMP packet that specifies that fragmentation is needed.
- 1 5. (Original) A method as recited in Claim 1, wherein the step of determining if the packet sequence value is valid comprises determining if the packet sequence value is within a range of packet sequence values that are allowed by the transport protocol for the connection.

1 6. (Original) A method as recited in Claim 1, wherein the step of determining if the  
2 packet sequence value is valid comprises determining if the packet sequence value is within a  
3 range of sent but unacknowledged TCP packet sequence values for the connection.

1 7. (Original) A method as recited in Claim 1, wherein the step of determining if the  
2 packet sequence value is valid comprises determining if the packet sequence value is exactly  
3 equal to one or more sequence values of one or more packets that are then-currently stored in  
4 a TCP re-transmission buffer, starting at a sequence value of a previously sent segment that  
5 resulted in receiving the ICMP packet.

1 8. (Original) A method as recited in Claim 1, wherein the steps are performed in a  
2 router acting as a TCP endpoint node.

1 9. (Original) A method as recited in Claim 1, wherein the steps are performed in a  
2 firewall device.

1 10. (Currently Amended) A method of preventing an attack on a network, the method  
2 comprising the computer-implemented steps of:  
3 receiving, at a TCP endpoint node in a TCP/IP packet-switched network, an ICMP  
4 packet that includes a copy portion of a TCP header associated with a TCP  
5 connection;  
6 obtaining a packet sequence number from the portion of the TCP header;  
7 determining if the packet sequence number is valid; and  
8 responding to the ICMP packet by updating a maximum transmission unit (MTU)  
9 value associated with the TCP connection only if the packet sequence number  
10 is determined to be valid.

1 11. (Original) A method as recited in Claim 10, wherein the step of receiving an ICMP  
2 packet comprises receiving an ICMP “endpoint unreachable” error packet.

1 12. (Original) A method as recited in Claim 10, wherein the step of receiving an ICMP  
2 packet comprises receiving an ICMP packet that specifies that fragmentation is needed.

1 13. (Original) A method as recited in Claim 10, wherein the step of determining if the  
2 packet sequence number is valid comprises determining if the packet sequence number is  
3 within a range of TCP packet sequence numbers that are allowed for the connection.

1 14. (Original) A method as recited in Claim 10, wherein the step of determining if the  
2 packet sequence value is valid comprises determining if the packet sequence number is  
3 within a range of sent but unacknowledged TCP packet sequence values for the connection.

1 15. (Original) A method as recited in Claim 10, wherein the step of determining if the  
2 packet sequence value is valid comprises determining if the packet sequence number is equal  
3 to one or more sequence numbers of one or more packets that are then-currently stored in a  
4 TCP re-transmission buffer, starting at a sequence value of a previously sent segment that  
5 resulted in receiving the ICMP packet.

1 16. (Original) A method as recited in Claim 10, wherein the steps are performed in a  
2 router acting as a TCP endpoint node.

1 17. (Original) A method as recited in Claim 10, wherein the steps are performed in a  
2 firewall device.

1 18. (Currently Amended) A computer-readable medium carrying one or more sequences  
2 of instructions, which instructions, when executed by one or more processors, cause the one  
3 or more processors to ~~carry out the steps of any of claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12,~~  
4 ~~13, 14, 15, 16, or 17~~ perform the steps of:

5 receiving an ICMP packet, wherein a data field within the ICMP packet includes a  
6 portion of a header associated with a connection in a connection-oriented  
7 transport protocol, and wherein the portion of the header includes a packet  
8 sequence value associated with the connection;  
9 obtaining the packet sequence value from the header;  
10 determining if the packet sequence value is valid; and  
11 responding to the ICMP packet by updating a parameter value associated with the  
12 transport protocol connection only if the packet sequence value is determined  
13 to be valid.

1 19. (Currently Amended) Apparatus for preventing an attack on a network, comprising:  
2 means for receiving an ICMP packet ~~that includes, wherein a data field within the~~  
3 ICMP packet includes a copy portion of a header associated with a connection  
4 in a connection-oriented transport protocol, and wherein the portion of the  
5 header includes a packet sequence value associated with the connection;  
6 means for obtaining [[a]] the packet sequence value from the header;  
7 means for determining if the packet sequence value is valid; and  
8 means for responding to the ICMP packet by updating a parameter value associated  
9 with the transport protocol connection only if the packet sequence value is  
10 determined to be valid.

1 20. (Currently Amended) An apparatus as recited in Claim 19, wherein the means for  
2 receiving an ICMP packet comprises means for receiving an ICMP packet that includes a  
3 copy portion of a TCP header associated with a TCP connection.

1 21. (Original) An apparatus as recited in Claim 19, wherein the means for receiving an  
2 ICMP packet comprises means for receiving an ICMP “endpoint unreachable” error packet.

1 22. (Original) An apparatus as recited in Claim 19, wherein the means for receiving an  
2 ICMP packet comprises means for receiving an ICMP packet that specifies that  
3 fragmentation is needed.

1 23. (Original) An apparatus as recited in Claim 19, wherein the means for determining if  
2 the packet sequence value is valid comprises means for determining if the packet sequence  
3 value is within a range of packet sequence values that are allowed by the transport protocol  
4 for the connection.

1 24. (Original) An apparatus as recited in Claim 19, wherein the means for determining if  
2 the packet sequence value is valid comprises means for determining if the packet sequence  
3 value is within a range of sent but unacknowledged TCP packet sequence values for the  
4 connection.

1 25. (Original) An apparatus as recited in Claim 19, wherein the means for determining if  
2 the packet sequence value is valid comprises means for determining if the packet sequence  
3 value is equal to one or more sequence values of one or more packets that are then-currently  
4 stored in a TCP re-transmission buffer.

1 26. (Original) An apparatus as recited in Claim 19, comprising a router acting as a TCP  
2 endpoint node.

1 27. (Original) An apparatus as recited in Claim 19, comprising a firewall device.

1 28. (Currently Amended) A network element, comprising:  
2 a network interface that is coupled to a data network for receiving one or more packet flows  
3 therefrom;  
4 a processor;  
5 one or more stored sequences of instructions which, when executed by the processor, cause  
6 the processor to ~~carry out the steps of any of claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14,~~  
7 ~~15, 16, or 17~~ perform the steps of:  
8 receiving an ICMP packet, wherein a data field within the ICMP packet includes a  
9 portion of a header associated with a connection in a connection-oriented  
10 transport protocol, and wherein the portion of the header includes a packet  
11 sequence value associated with the connection;  
12 obtaining the packet sequence value from the header;  
13 determining if the packet sequence value is valid; and  
14 responding to the ICMP packet by updating a parameter value associated with the  
15 transport protocol connection only if the packet sequence value is determined  
16 to be valid.

1 29. (New) A network element as recited in Claim 28, wherein the step of receiving an  
2 ICMP packet comprises receiving an ICMP packet that includes a portion of a TCP header  
3 associated with a TCP connection.

1 30. (New) A network element as recited in Claim 28, wherein the step of receiving an  
2 ICMP packet comprises receiving an ICMP “endpoint unreachable” error packet.

1 31. (New) A network element as recited in Claim 28, wherein the step of receiving an  
2 ICMP packet comprises receiving an ICMP packet that specifies that fragmentation is  
3 needed.

1 32. (New) A network element as recited in Claim 28, wherein the step of determining if  
2 the packet sequence value is valid comprises determining if the packet sequence value is  
3 within a range of packet sequence values that are allowed by the transport protocol for the  
4 connection.

1 33. (New) A network element as recited in Claim 28, wherein the step of determining if  
2 the packet sequence value is valid comprises determining if the packet sequence value is  
3 within a range of sent but unacknowledged TCP packet sequence values for the connection.

1 34. (New) A network element as recited in Claim 28, wherein the step of determining if  
2 the packet sequence value is valid comprises determining if the packet sequence value is  
3 exactly equal to one or more sequence values of one or more packets that are then-currently  
4 stored in a TCP re-transmission buffer, starting at a sequence value of a previously sent  
5 segment that resulted in receiving the ICMP packet.

1 35. (New) A network element as recited in Claim 28, wherein the steps are performed in  
2 a router acting as a TCP endpoint node.

1 36. (New) A network element as recited in Claim 28, wherein the steps are performed in  
2 a firewall device.